National Infrastructure Protection Center CyberNotes

Issue #2000-04 *March 8, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 11 and February 24, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BTT Software[1]	SNMP Trap Watcher Version 1.16	A vulnerability exists which allows a remote malicious user to crash the trap watcher without being logged.	Patch available at: http://www.bttsoftware.co.uk/cgi-bin/download.cgi?download/snmptrap.zip	SNMP Trap Watcher Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Debian[2]	GNU/Linux 2.1	The make package which is shipped in Debian GNU/Linux 2.1 is vulnerable to a race condition that can be exploited with a symlink attack.	This has been fixed in version 3.77-5slink. We recommend you upgrade your make package immediately. Download updated packages: http://security.debian.org/dists/stable/updates	Debian Make Race Condition	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Securiteam, February 10, 2000.
[2] Debian Security Advisory, February 20, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[3]	DeleGate 5.9.13 and prior; 6.0.9 and prior	An optional third-party port, DeleGate, when distributed with FreeBSD contains numerous remotely exploitable buffer overflows, which allow malicious users to execute arbitrary code on the local system.	Workaround: Remove the DeleGate port/package.	DeleGate Security buffer overflow	**High**	Bug discussed in newsgroups and websites.
FreeBSD[4]	FreeBSD 3.0-3.4	Two optional third-party ports, ASCPU and ASMON, distributed with FreeBSD can be used to execute commands with elevated privileges This may lead to a local root compromise.	FreeBSD has released a new ports package for these applications which can be downloaded from: http://www.si.freebsd.org/es/ports/sysutils.html	FreeBSD ASMON/ ASCPU privilege elevation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
FTPx[5]	FTP Explorer 1.0.00.10	FTP Explorer includes the option to store profiles of visited FTP sites. The user's name and password can also be stored encrypted but the encryption mechanism is weak and can easily be broken.	No workaround or patch available at time of publishing.	FTPx FTP Explorer Weak Password Encryption	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[6]	HP-9000 Series 700/800 running release HP-UX 11.x	Trusted systems may have vulnerabilities if the password field in /etc/passwd is blank.	Verify that all entries in /etc/passwd have "*" in the password field if the system is trusted.	Trusted Systems Password	Medium	Bug discussed in newsgroups and websites.
Hewlett-Packard[7] ***HP-UX 11.04 is also vulnerable[8]***	**HP-UX 11.0, 10.30**	**A vulnerability exists in the Maximum Path MTU (PMTU) procedure that allows it be used as a packet amplifiers.**	**Workaround: Set the NDD parameter ip_pmtu_strategy to 1.** ***HP's recommended solution is available at:*** http://localhost/archives/bugtraq/current/0112.html	**PMTU Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
Infopop Corp.[9]	Ultimate Bulletin Board 5.43	A remote malicious user can retrieve any file the perl CGI script has access to. It is also possible to execute arbitrary commands on a server running UBB.	This vulnerability was verified to have been fixed in the shareware version (and presumably the commercial as well).	Ultimate Bulletin Board Perl CGI Security Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[3] FreeBSD Security Advisory, SA-00:04, February 19, 2000.
[4] FreeBSD Security Advisory, SA-00:03, February 19, 2000.
[5] SecurityFocus, February 25, 2000.
[6] Hewlett-Packard Security Advisory, 00111, February 17, 2000.
[7] Hewlett-Packard Security Advisory, HPSBUX0001-110, January 24, 2000.
[8] Network Computing Security Express #032, February 17, 2000.
[9] Bugtraq, February 13, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Internet Software Consortium (ISC)[10]	Bind 8.2-8.2.2, 4.9.7-T1B, 4.9.7, 8.1-8.1.2; Multiple DNS Servers	A potential Denial of Service vulnerability exists in the default configuration of many popular DNS servers. If a server allows for remote hosts to query it for hosts other than those it serves, causing recursion, it may be possible to cause traffic amplification.	Administrators should not allow recursive queries from their nameservers, except from a trusted host or network. For bind, the option to set is the "allow-query" option. By setting this to a list of hosts or networks allowed to query recursively, you can prevent their servers from being used as an amplification site.	Nameserver Traffic Amplification and NS Route Discovery	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[11]	FrontPage Personal WebServer 3.0.2.926	Front Page Personal Web Server will follow '/..../' strings in requested URLs, allowing remote malicious users to obtain unauthenticated read access to files/directories on the same logical drive as the web content. Hidden files are viewable, although the Front Page directory itself is not. The user must know the name and path of the desired file.	No workaround or patch available at time of publishing.	Microsoft FrontPage PWS Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[12]	Internet Explorer 4.0, 4.01, 5, 5.01	A security vulnerability exists in Internet Explorer, which could allow a malicious web site operator to read – but not add, change or delete – certain types of files on the computer of a visiting user.	Patch available at: http://www.microsoft.com/windows/ie/security/patch5.asp	Image Source Redirect	Medium	Bug discussed in newsgroups and websites.

[10] TESO Security Advisory, February 11, 2000.
[11] Bugtraq, February 16, 2000.
[12] Microsoft Security Bulletin, MS00-009, February 16, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[13] ***Microsoft has released a patch for this vulnerability.***[14]	**Internet Explorer 4/5** ***All builds in the 2000, 3100, and 3200 Series***	**A security vulnerability exists in Microsoft's Java Virtual Machine, which allows a Java applet to read files in certain directories. This can be done via the getSystemResourceAsStream() function.**	**No workaround or patch available at time of publishing.** ***This vulnerability is quite dangerous and immediate de-activation of IE's Java functionality provided by Microsoft VM is highly recommended.*** ***2000 Series:*** www.microsoft.com/java/vm/dl-vmsp2.htm ***3000 Series:*** www.microsoft.com/java/vm/dl-vm32.htm ***3200 Series:*** www.microsoft.com/java/vm/dl-vm40.htm	**Microsoft Java Virtual Machine GetSystem ResourceAs Stream**	**Very High**	**Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.**
Microsoft[15]	Outlook Express 4.27.3110.1, 4.72.2106.4, 4.72.3120.0, 4.72.3612.1700 Outlook Express 5.0; Outlook 98/2000; Internet Explorer 4x, 5x	The Active Setup ActiveX control can be configured to notify the user when a component signed by a trusted vendor is installed. Even when this feature is enabled, when the component is signed by Microsoft no notification is provided. This 'feature' could be exploited remotely via a web page or HTML email.	No workaround or patch available at time of publishing. Microsoft will be modifying the Active Setup control so that it warns before downloading unless a customer has specifically requested that he not be warned in the future.	Microsoft Signed ActiveX Active Setup	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Microsoft[16]	Site Server 3.0 Commerce Edition	Two sample web applications that ship with Site Server 3.0 Commerce Edition and the code generated by an included Site Wizard do not properly filter incoming user data, which would allow a malicious user to run arbitrary SQL commands.	Patch available at : http://www.microsoft.com/downloads/Release.asp?ReleaseID=18767	MS Site Server Commerce Edition Input Validation	**High**	Bug discussed in newsgroups and websites.
Microsoft[17]	Systems Management Server 2.0	A security vulnerability exists in the installation routine associated with Microsoft Systems Management Server (SMS). If particular features have been enabled, the vulnerability could allow a malicious user to gain elevated privileges.	Patch available at: X86: Http://www.microsoft.com/Downloads/Release.asp?ReleaseID=18498 Alpha: http://www.microsoft.com/Downloads/Release.asp?ReleaseID-18499	Remote Agent Permissions	Medium	Bug discussed in newsgroups and websites.

[13] Bugtraq, February 1, 2000.
[14] Microsoft Security Bulletin, MS00-011, February 19, 2000.
[15] Bugtraq, February 19, 2000.
[16] Microsoft Security Bulletin, MS00-010, February 18, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[18]	Windows 2000	During the install procedure for Windows 2000, the ADMIN$ share file is created. However, the Administrator password, although entered, is not activated until after the next reboot. Therefore, during this period of time, it is possible for anyone with network access to the machine to connect to the share as Administrator with no password.	No workaround or patch available at time of publishing.	Microsoft Windows 2000 Install Unprotected ADMIN$ Share	Medium Note: This may be **High** risk in some installa-tions	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[19]	Windows 95/98/NT	The autorun feature in Windows allows local malicious users to gain higher privileges. This can be done by creating a file at the root of any removable media (such as CDs, Zip Drive diskette, removable hard drives, etc.) and waiting for a privileged user to browse the affected drive with the Explorer program.	Workaround: Disable the autorun feature by adjusting the following registry key: HKEY_CURRENT_USER\ Software\Microsoft\Windows\ Current version\Policies\Explorer\ NoDriveTypeAutoRun. You should change the value to OxFB, which will limit the autorun feature to the local DDROM drive.	Microsoft Windows Autorun.inf Privilege Escalation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[20]	Windows Media Services 4.0, 4.1	A security vulnerability exists which could allow Denial of Service attack against a streaming media server. Misordered handshake sequences sent to a Windows Media Unicast Server via Windows Media Player will cause the server to crash.	Microsoft has released patches for this issue, available at: Windows NT Server 4.0: http://download.microsoft.com/download/winmediatech40/Update/4954/NT4/EN-US/WMSU4954_NT4.exe Windows 2000 Server: http://download.microsoft.com/download/winmediatech40/Update/4954/NT5/EN-US/WMSU4954_Win2000.exe	Microsoft Windows Media Services Handshake Sequence DoS	Low	Bug discussed in newsgroups and websites.
Microsoft[21]	Windows NT Server 4.0 with Internet Information Server 4.0	A remote Denial of Service vulnerability exists in the InetInfo.exe when a long filename under the \mailroot\pickup directory is created	No workaround or patch available at time of publishing.	InetInfo.Exe Denial of Service	Low	Bug discussed in newsgroups and websites.

[17] Microsoft Security Bulletin, MS00-012, February 22, 2000.
[18] Bugtraq, February 15, 2000.
[19] Bugtraq, February 18, 2000.
[20] Microsoft Security Bulletin, MS00-013, February 23, 2000.
[21] Securiteam, February 21, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[22]	Multiple Vendors (3COM, Cray, HP, Sun/Sparc, Windows, etc.)	In a number of network devices/operating systems default communities exist which are world writeable. By being world writeable, they allow remote users to configure properties of the device/OS without any authorization other than knowledge of the community name.	A permanent fix is to change or remove the default communities. A workaround is to disable SNMP access. Sun's Solaris protected against this in version 2.7. Microsoft addressed this problem for Windows NT 4.0 in Service Pack 4, SNMP is disabled by default.	Multiple Vendor SNMP World Writeable Community	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
NetBSD[23]	NetBSD 1.4.1 and prior; NetBSD-current until 20000126	A vulnerabilty exists in the proc filesystem, which allows any user to become root.	A patch is available for NetBSD 1.4.1, located at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/20000130-procfs NetBSD-current since 20000126 is not vulnerable. Users of NetBSD-current should upgrade to a source tree later than 20000126.	NetBSD Procfs Security	**High**	Bug discussed in newsgroups and websites.
NetBSD[24]	NetBSD/vax 1.4.1 and earlier; -current prior to 19991212	A wrapper program can be constructed by a malicious local user that can modify the hardware privileges of a ptrace(2)'d process. It might be possible to write a security-related exploit via this mechanism.	Upgrade to NetBSD-current, or apply the patch to 1.4.1, which is listed in the Security Advisory.	Ptrace(2)'d Hardware Privileges	Medium	Bug discussed in newsgroups and websites.
Netopia[25]	Timbuktu Pro Remote Control 5.2.1, 2.0	Simple connections and disconnections to Timbuktu ports can hang the authentication process and halt all Timbuktu services. The vulnerability also exists on the 5.2.1 Macintosh platform.	No workaround or patch available at time of publishing.	Netopia Timbuktu Pro 2.0 Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Novell[26] ***Novell has released a patch[27]***	**Border Manager 3.0, 3.5**	**A security vulnerability exists which enables malicious users to perform a Denial of Service attack against the firewall, causing it to stop responding.**	**Workaround: Unload the CSATPRX.NLM or block incoming requests to port 2000 from the external interface.** **The patched ctaspxy1.exe is available at:** http://support.novell.com	**Novell Border Manager Audit Trail Proxy DoS**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[22] SecurityFocus, February 15, 2000.
[23] NetBSD Security Advisory, 2000-001, February 19, 2000.
[24] NetBSD Security Advisory, 1999-012, February 16, 2000.
[25] Bugtraq, February 15, 2000.
[26] SecurityFocus, February 4, 2000.
[27] Network Computing Security Express #032, February 17, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Pragma Systems[28]	InterAccess TelnetD Server 4.0	The code that handles the login commands in the telnet session has an buffer overflow that may allow a malicious user to gain access.	Pragma System has stated that their current version is Build 7, which does not appear to contain the buffer overflow condition.	InterAccess TelnetD Server 4.0 Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Pragma Systems[29]	InterAccess TelnetD Server 4.0	Sending invalid, unexpected characters in the client's terminal configuration settings can crash the Pragma Systems InterAccess TelnetID Server 4.0. This causes telnetd.exe to GPF, and causes the server to stop responding.	Pragma Systems has released a new version of InterAccess TelnetD Server, Build 8, which rectifies this issue. It is available for download at the following website: http://www.pragmasys.com/TelnetD/	InterAccess TelnetD Server 4.0 Terminal Configuration	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sambar[30]	Server 4.2beta 7 and older	A vulnerability exists in the Sambar Web/FTP/Proxy Server for Windows NT/2000 cgi-bin directory which could be used by a remote malicious user to run any valid command-line program with Administrator privileges.	Sambar Technologies has made available a version of Sambar Server that does not ship with any batch files. However, batch file execution is still supported and therefore the machine is still compromisable if batch files are uploaded to the cgi-bin by any means. The batchless version (4.3 Beta 8) may be downloaded from the location below: http://www.sambar.com/beta.htm	Sambar Server Batch CGI	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SCO[31]	OpenServer 5.0-5.0.5	An implementation fault in MMDF allows arbitrary individuals to obtain mail management privileges via the SMTP daemon. A malicious user can subsequently gain root access. This vulnerability is specific to the version of MMDF shipped from SCO	SCO has made patches available for this issue which can be found at: http://www.sco.com/security	SCO MMDF Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SCO[32]	Unixware 7.1, 7.1.2	An implementation fault in the ARCserve agent script allows local malicious users to obtain root privileges.	SCO has made patches available for this problem which can be found at: http://www.sco.com/support	SCO Unixware ARCserver /tmp symlink	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[28] USSR Labs Advisory Code, USSR-2000033, February 22, 2000.
[29] USSR Labs Advisory Code, USSR-2000034, February 24, 2000.
[30] SecurityFocus, February 24, 2000.
[31] Network Associates, Inc. Security Advisory, NAI-Feb152000-2: February 15, 2000.
[32] Network Associates Inc. Security Advisory, NAI-Feb152000, February 15, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun and other products which use the FlexLM license management system[33]	GLOBEtrotter FLEXlm 6.1; Sun Workshop 5.0; Sun Solaris 2,6, 2.6_X86; 2.7, 2.7_X86	A vulnerability exists in the installation of licenses for Sun's WorkShop 5.0 compilers, and other products, which use the FlexLM license management system. As part of the installation process, the 'lit' program is run. This program insecurely creates files in /var/tmp, which can be used to create files owned by root, with known contents. These file will be created with root's umask, which by default is 0022.	No workaround or patch available at time of publishing.	FlexLM Symlink	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
T.C.X DataKonsult [34] ***Exploit code has been released.[35]***	**MySQL 3.22.26-3.22.29, 3.23.8-9**	**A vulnerability exists in the password verification scheme, which will allow any user on a machine that has been granted access to the database. This access is granted without knowing the account name or password of the user.**	**No workaround or patch available at time of publishing.** ***No current MySQL is vulnerable to this exploit.***	**MySQL Unauthenticated Remote Access**	**Medium**	**Bug discussed in newsgroups and websites.** ***Exploit has been published.***

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 11 and February 24, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security**

[33] SecurityFocus, February 21, 2000.
[34] SecurityFocus, February 9, 2000.
[35] Securiteam, February 18, 2000.

vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing. During this period, 57 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
February 24, 2000	Whatuneed.txt	Technique described for spoofing/hijacking/predicting sequence numbers for executing TCP/IP attacks.	
February 24, 2000	Wordpad-ie.txt	Demonstration code for exploiting the Wordpad vulnerability in Internet Explorer.	
February 23, 2000	Dostelnetd.exe	Exploit code for the InterAccess Telnet Server vulnerability.	
February 22, 2000	Madscan.c	Scans for sites, which do not block broadcast IP addresses.	
February 22, 2000	Noob.zip	An Active X Trojan horse that is controlled via IRC.	
February 22, 2000	Scs.zip.	Windows based CGI scanner.	
February 22, 2000	**Sftpd-scan.tar**	**Exploit for the WU-FTPD 2.5 overflow.**	
February 22, 2000	Spurf.c	A mail-like smurf that uses mail relays instead of broadcasts.	
February 22, 2000	Trypop3.c	Code that attempts to overflow user/password variables.	
February 21, 2000	Adore-0.14.tar.gz	A Linux LKM based rootkit which features PROMISC flag hiding, persistent file and directory hiding, process-hiding, netstat hiding, rootshell-backdoor, and an uninstall routine. Includes a userspace program to control everything.	
February 21, 2000	Ebpd.tgz	Script which sniffs traffic on the networking watching for Ebay userids and passwords. .	
February 21, 2000	**ftp-ozone.c.txt**	**Exploit for recent FW-1 FTP vulnerabilities.**	
February 21, 2000	Roi.sh	Shell script, which remotely identifies operating systems using Netcraft's services.	
February 18, 2000	md-webscan-1.0.0.tar.gz	CGI vulnerability scanner that easily extensible.	
February 18, 2000	**Snmp.writable.txt**	**A list of devices with default writable configurations, which allow a malicious user to modify routing tables, status of network interfaces, and other vital system data.**	
February 18, 2000	Vanish2.tgz	Log wiper that cleans WTMP, UTMP, astlog, messages, secure, xferlog, maillog, warn, mail, httpd.access_log and httpd.error_log.	
February 17, 2000	Decss.tar.gz	A perl script that removes CSS tags from HTML pages.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
February 17, 2000	Nessus-0.66.5-1.tgz	A remote security scanner for Linux, BSD, Solaris and some other systems which is multithreaded, plugin-based, and has a GTK interface and performs over 320 remote security checks.	
February 17, 2000	NSS-2000pre7.tar.gz	Narrow Security Scanner 2000 searches for 297 remote vulnerabilities, which is written in Perl and tested on RedHat, FreeBSD, OpenBSD, Slackware, and SuSE.	
February 17, 2000	Spidermap-0.1.tar.gz	A collection of perl scripts that enables you to launch precisely tuned network scans.	
February 16, 2000	**Adv3.tar.gz**	**Nameserver traffic amplify (DNS Smurf) and NS route discovery (DNS Tracerroute) advisory and exploit.**	
February 16, 2000	**Hv-smtpdos.pl**	**Perl script which sends many mails to a list of addresses to test for the SMTP vulnerabilities.**	
February 16, 2000	Icmpenum-1.1.tgz	A proof-of-concept tool that demonstrates possible distributed attacking concepts.	
February 16, 2000	Rcgixploit.c.txt	Remote CGI exploit which attempts to exploit five common CGI vulnerabilities and retrieves /etc/passwd.	
February 16, 2000	Rpv21.tar.gz	A tool, which allows you to telenet backward through a firewall, assuming the box is allowed to make outgoing tcp connections.	
February 16, 2000	Teso-nxt.tar.gz	Exploit for the BIND-8.2/8.2.1 NXT vulnerability.	
February 15, 2000	Adore-0.13.tar.gz	Linux LKM based rootkit.	
February 15, 2000	Decrypt.zip	This is a Windows application that displays the password for Sybergen Secure Desktop.	
February 15, 2000	Hellkit-1.1.tar.gz	Shellcode generator that lets you write your code in C and then converts it to ASM for use with both heap and stack based overflows.	
February 15, 2000	Localscan.tar.gz	A perl-based frontend for nmap.	
February 15, 2000	Vanish.c	Log wiper that cleans WTMP, UTMP, astlog, messages, secure, xferlog, maillog, warn, mail, httpd.access_log and httpd.error_log.	
February 15, 2000	Voideye.zip	A Windows 9x/NT/2000 SCI scanner that scans for 119 known vulnerabilities.	
February 15, 2000	**Wu-ftpd-trojan.tar.gz**	**WU-FTPD Trojan.**	
February 11, 2000	3wahas.tar.gz	LAN based SYN flooder, which spoofs SYN ACK packets and allows them to bypass SYN-cookies.	
February 11, 2000	Adv1.tar.gz	Linux 2.2.x ISN vulnerability advisory and exploit.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
February 11, 2000	Arptool-0.0.1.tar.gz	Send arp packets useful for the man-in the middle attack.	
February 11, 2000	Ascend-foo.c	Denial of Service ascend router with simple udp echo<->echo link.	
February 11, 2000	**Delefate.c**	**Delegate 5.9.x-6.0.x remote exploit for Linux compilations.**	
February 11, 2000	Dirthy.c	Linux TTY hijacker.	
February 11, 2000	Fizzbounce-0.2.tar.gz	Maps connections over HTTP proxies.	
February 11, 2000	Grabbb-0.1.0.tar.gz	Fast functional banner scanner.	
February 11, 2000	**Ifafoffuffoffaf.c**	**Wu-FTPD 2.5.0 heap-based exploit.**	
February 11, 2000	Itunnel-1_2.tar.gz	ICMP tunneling tool.	
February 11, 2000	Lamescan-1.0.tar.gz	A simple threaded port scanner5.	
February 11, 2000	Libtermcapsploit.c	Libtermcap exploit.	
February 11, 2000	Lrk5.scr.tar.gz	Linux rootkit 5 that contains backdoor versions of chfn, chsh, crontab, du, find, ifconfig, inetd, killall, linsniffer, login, ls, netstat, passwd, pidof, ps, rshd, syslogd, tcpd, top, sshd, and su.	
February 11, 2000	Mailbrute.c	Sendmail brute forcer that looks for valid accounts. Uses the RCPT command.	
February 11, 2000	Numby-0.2.tar.gz	Scans for relay vulnerable HTTP proxies.	
February 11, 2000	Phoenix.tar.gx	Shoots every TCP connection in the LAN by spoofing TCP packets.	
February 11, 2000	Phoenix2.tar.gz	Shoots every TCP connection in the LAN by spoofing TCP packets and also spoofs the MAC address.	
February 11, 2000	Pro.tar.gz	Proftpd exploit for 1.2.0pre3 Linux x86.	
February 11, 2000	Proftp-ppc.c	Proftpd Linux ppc remote exploit.	
February 11, 2000	Rcpt-analisys.tgz	Includes demonstration code lsmtp-cracker.c.	
February 11, 2000	Realown.c	Unix-port of the RealServer exploit.	
February 11, 2000	Sendm-8.0.3.trojan.tar.gz	Backdoored Sendmail 8.9.3 that lets you enter a special SMTP command and it opens a root shell.	
February 11, 2000	Tesoiis.c	Port of the eeye IIS4 exploit.	
February 11, 2000	Vwxploit.c	Interscan Virus Wall 3.23/3.3 exploit.	
February 11, 2000	Zylyx-0.1.1.tar.gz	HTTP proxy-cache file finder that goes through http proxies from a file and requests a file.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two-week period:

TROJ_TRINOO is the latest addition of daemon agents that allows malicious users to access your computer and use it in a Denial of Service attack on another network. TROJ_TRINOO can function in a Windows environment and it can also be sent by email like other viruses and Trojans. The vast number of PCs connected to the Internet, now able to be used in DDoS attacks, raises the threat level substantially.
There has been an increase in intruders attempting to compromising systems and install Distributed Denial of Service (DDoS) tools, such as Trin00, TFN, TFN2K, or Stacheldraht, for launching packet-flooding Denial of Service attacks. More information regarding these type of attacks may be found at the CERT or NIPC web sites: http://www.cert.org and http://www.nipc.gov respectively. One of the ways organizations can assist in stopping these DDoS attacks is to place egress filters on their gateways. A SANS paper on egress filtering can be found at http://www.sans.org/y2k/egress.htm

Melissa, the worm that hit the headlines towards the end of March 1999 when it infected thousands of computers via the Internet, has resurged.
There has been an increase in systems being compromised via the WU-FTP or WU-FTPD vulnerabilities. There has been an increase in systems being root compromised via the 'NXT' vulnerability in BIND. Also, numerous systems are being root compromised via the sadmind (port 111 - sunrpc) vulnerabilities.
Increases in SSH attack attempts.
There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337.
A Denial of Service attack tool, stream.c, has been discovered which could cause Unix machines to stop responding. It floods the host with ACK's coming from random IPs with remote sequence numbers. This type of attack may be difficult to filter out as it may resemble "normal" traffic.
A new Windows 9x Denial of Service named twinge.c has been made available. The DoS sends all possible types of ICMP traffic, making Windows 9.x systems crash immediately.
Deployment of password stealing Trojans, attacking AOL users, has reportedly been on the rise.
The newly discovered Poison Null and Upload Bombing security attacks could let crackers cripple many interactive websites. Both attacks exploit vulnerabilities in CGI programs that translate between the HTML used in Web pages and the servers that run interactive websites.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each

month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as updates become available**. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections during the last three months reported), and approximate date first found.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of 175 distinct viruses are currently consider "in the wild" by anti-virus experts. In the wild viruses have been reported to anti-virus vendors by their clients and have infected user machines.

Viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date
1	W95 CIH	File	Slight increase	August 1998
2	W97M Marker	Macro	Slight increase	April 1999
3	W97M Melissa.A	Macro	Increase	April 1999
4	W97M Ethan.A	Macro	Steady	February 1999
5	W32/SKA (aka Happy 99)	File	Decrease	March 1999
6	W97M Class.D	Macro	Slight decrease	December 1998
7	W32 PrettyPark	File	New to table	June 1999
8	W32 ExploreZip	Worm	New to table	June 1999
9	WM CAP.A	Macro	Slight decrease	May 1997
10	O97M Tristate.C	Macro	Slight decrease	April 1999

W97M/Eight941D (Word 97 Macro Virus): This virus infects Word 97 documents as well as the global template the application uses.

On July 1st and/or November 10th, the virus carries out the following malicious actions on the Word documents it detects: all Word documents opened will no longer appear in the Recent Files list; when a Word document is changed and then saved, the virus will instruct Word to save only the changes you have made; the virus prevents you from making a backup copy of documents; you will no longer be asked if you want to save the template when this has been changed; and the password "xyz" is assigned to each document.

W95/Fabi.9608 (Windows 95/98 Multipartite Virus): This virus infects executable files (programs) in Windows 95/98, as well as Word documents and the global template this application uses. The virus is encrypted and it infects EXE files in the current folder in the C:\Windows and C:\Windows\System directories.

Infection routines are carried out in different ways depending on where it is executed and what kind of files it is infecting. It spreads very quickly but has no destructive effect. To propagate, the virus uses the EXE files it infects, as well as infected Word documents and/or the global Word template, NORMAL.DOT. The way the virus infects also depends on the operating system on which it is run.

WM97/Marker-BQ (Word 97 Macro Virus): This virus has been reported in the wild and has two potential payloads.

On the first day of the month it appends information about the infected user to the virus macro. Because of this it is possible to view a log of who has been infected.

The second payload of the virus is delivered on Sundays and it overwrites several important settings in the Windows registry. The overwritten settings are:

> ProductKey, ProductId, ProductName, ComputerName,
> RegisteredOrganization,
> RegisteredOwner and Version.

ProductKey is overwritten with "D4EST-R9OY9-6ORY9-O9U68-RS2X3"
ProductID is overwritten with "10701-000-1090706-02120"
ProductName is overwritten with "Jon has conquered your Program hehehe"
ComputerName is overwitten with "Jonhehehe"
RegisteredOrganization is overwritten with "Ngentot Terus"
RegisteredOwner is overwritten with "jonhehehe Tentu"
CurrentVersion is overwritten with "Destroy Everyting u see by Jon"

The virus then attempts to run a program called SCANREG.EXE and contains some text, which does not get displayed:

> This log file is created to have a story for you about my virus travel.
> any comment and suggestion call 62+2%!-245%0% or email to
> jonhehehehe@ho####.com

WM97/Melissa-AB (Word 97 Macro Virus): This virus is based upon several Word macro viruses, the main one being WM97/Melissa.

Upon closing an infected document the virus does the following:

> In December, if the day of the month is greater than the 23rd,
> the virus displays a message box asking:
>
> "I wish you a Merry X-mas!! Do you love me?"
>
> If you answer "Yes" the virus responds with
>
> "Thank You! I Love You. You are so cute."
>
> If you answer "No" the virus responds with:
>
> "You are so rude."
> "Fuck you, Asshole!"

The virus then forwards itself to the first 15 addresses in your mail address book:

> Subject: An important advice from
>
> Message text: Take a look in this Document, urgent
> suggestions to be a cool man!! ;-)

The currently opened document is attached.

On January 1st the virus displays the message:

> "Happy New Year!!"

On the 28th or 29th of February it displays the messsage:

"It's Kouki's Birthday!"

Also upon opening of an infected document the virus disables all the menus in Word. To recover from this payload delete your NORMAL.DOT global template.

XM97/Laroux-DZ (Excel 97 Macro Virus): The virus has been reported in the wild and is a variant of the XM97/Laroux Excel macro virus.

It contains two macros, AUTO_OPEN and CK_FILES. The AUTO_OPEN macro is run when the infected document is opened, and instructs Excel to call the CK_FILES macro every time a new worksheet is activated.

When this happens, the virus creates a file in the XLSTART directory called RESULTS.XLS and copies the viral macros into it. This file is automatically opened every time Excel is run, much like Word's NORMAL.DOT. From then on it infects every workbook used.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

No new Trojan additions to this issue of CyberNotes.

Trojan	Version	Issue discussed
AOL Trojan		CyberNotes-2000-01
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
FakeFTP	Beta	CyberNotes-2000-02
Hack'A'tack	1.0-2000	CyberNotes-2000-01
InCommand	1.0-1.4	CyberNotes-2000-01
Intruder		CyberNotes-2000-01
Kuang Original	0.34	CyberNotes-2000-01
Matrix	1.4-2.0	CyberNotes-2000-01
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02